Ethical Hacking: La Importancia de una intrusión controlada

Manuel Henry Sanchez Carvajal
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
henrisito_hsc@hotmail.com

RESUMEN

El crecimiento exponencial del internet ha traído muchas cosas buenas y ha revolucionado la forma en que interactuamos con el mundo pero como en la mayoría de los avances tecnológicos, hay también un lado oscuro: los hackers criminales. Los gobiernos, compañías y ciudadanos particulares alrededor del mundo están ansiosos por ser partícipes de esta revolución pero tienen miedo de que algún hacker irrumpa en su servidor web y distorsione su información, lea sus correos electrónicos, robe sus números de tarjeta de crédito de un sitio de compras en línea o implante algún software capaz de transmitir discretamente los secretos de su organización a la red abierta. Para hacer frente a estas preocupaciones tenemos a los hackers éticos, los cuales son fundamentales para asegurar que la información de la organización esté lo más resguardada posible. La importancia de realizar una prueba de intrusión controlada es más que evidente ya que un hacker ético emplea las mismas herramientas y técnicas que los intrusos para determinar posibles brechas de seguridad, esto también implica que se generan beneficios, algunos de los cuales son: luchar contra el terrorismo, tener un sistema preventivo contra intrusiones de hackers maliciosos e implementar medidas para evitar una brecha de seguridad.

Términos Generales

Medición, Confiabilidad, Seguridad, Factores Humanos, Experimentación, Verificación.

Palabras Clave

Brechas de seguridad, ventajas, desventajas, intrusiones.

1. INTRODUCCION

Con el rápido crecimiento de las tecnologías de Internet, la seguridad informática se ha vuelto una preocupación mayor para los gobiernos y empresas, donde la posibilidad de ser hackeado es proporcional a la seguridad implementada en su estructura.

Además, los posibles clientes de los servicios provistos por estas entidades están preocupados por la forma en que se gestiona su información personal que puede variar desde números de seguro social, números de tarjeta de crédito a direcciones domiciliarias.

En un esfuerzo para encontrar una solución apropiada al problema, las organizaciones se dieron cuenta que la mejor solución al problema es evaluar la amenaza de intrusión para lo cual se contratan a profesionales en seguridad informática para que intenten irrumpir en sus sistemas computacionales. Tal solución es similar a tener auditores independientes para verificar los estados de libros de una organización.

Con el mismo concepto, el equipo profesional de seguridad (hackers éticos) empleará las mismas herramientas y técnicas usadas por intrusos para investigar las brechas de seguridad y vulnerabilidades sin dañar o robar datos del sistema en cuestión.

Una vez terminado el proceso, el equipo de seguridad reportará a los propietarios las vulnerabilidades que encontraron y las instrucciones sobre cómo eliminar dichas brechas de seguridad.

2. IMPORTANCIA

La evaluación de la seguridad de un sistema por parte de un hacker ético busca responder 3 preguntas básicas:

- ¿Qué puede ver un intruso en los sistemas atacados?
- ¿Qué puede hacer un intruso con esa información?
- ¿Hay alguien en el sistema atacado que se dé cuenta de los ataques o éxitos del intruso?

De hecho la primera y segunda pregunta son importantes pero la más importante es la tercera: Si los propietarios u operadores del sistema atacado no se dan cuenta que alguien está tratando de irrumpir, los intrusos pueden y pasarán semanas o incluso meses intentando acceder al sistema, lo cual eventualmente lograrán.

Cuando el cliente solicita una evaluación, hay bastante documentación y discusiones que realizar. La discusión empieza con las respuestas del cliente a preguntas similares a las propuestas por Garfinkel y Spafford:

1. Qué está tratando de proteger?
2. Contra qué trata de proteger?
3. Cuanto tiempo, esfuerzo y dinero está dispuesto a gastar para obtener protección adecuada?

Un sorprendente número de clientes tienen problemas para responder con precisión la primera pregunta: un centro médico diría “la información de nuestros pacientes”, una firma de ingenieros respondería “nuestros nuevos diseños de productos” y un minorista en la Web diría “nuestra base de datos de clientes”.

La respuesta para (1.) debe contener más que solo una lista de recursos de información en la computadora de la organización. El nivel de daño a la buena imagen de una organización, como resultado de una intrusión criminal exitosa, puede variar de

ligeramente embarazoso a una seria amenaza a la rentabilidad. Como ejemplo de una intrusión que afectó a la imagen de una organización, el 17 de enero del año 2000 una página web de la Biblioteca del Congreso de EE.UU. fue atacada, a continuación se muestra tanto la pantalla inicial como la pantalla hackeada después del ataque:

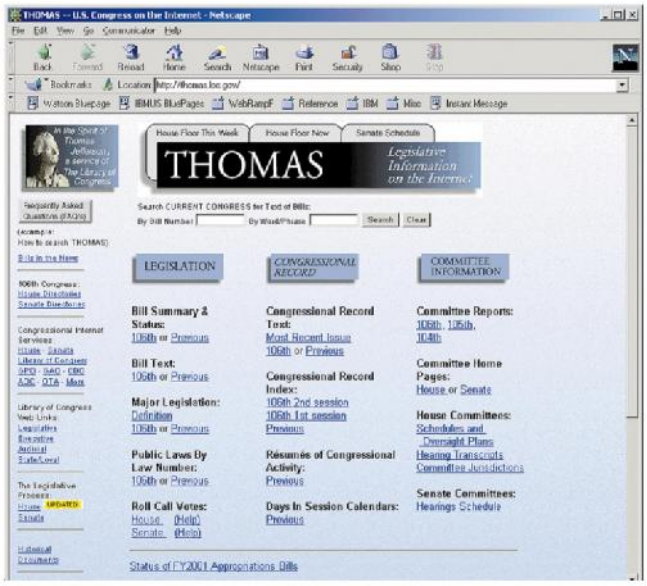

Fig.1 Página Web antes del ataque

Fig. 2 Página Web después del ataque

Algunos clientes tienen la errónea impresión de que sus sitios web no serán un objetivo. Pueden citar numerosas razones, como "mi página web no tiene nada interesante" o "los hackers nunca han escuchado de mi compañía". Lo que estos clientes no se dan cuenta es que *todos los sitios web son un objetivo*. El objetivo de muchos hackers criminales es sencillo: hacer algo espectacular y luego asegurarse que todos sus camaradas se enteren. Otro argumento es que a muchos hackers simplemente no les importa de qué organización o compañía se trate; ellos hackearan tu sitio web *porque pueden*. Por ejemplo, los administradores Web en UNICEF debieron pensar que ningún hacker los atacaría. Sin embargo en Enero de 1998 su página fue desfigurada (figuras 3 y 4).Muchos otros ejemplos de ataques por parte de hackers pueden encontrarse por toda la Web.

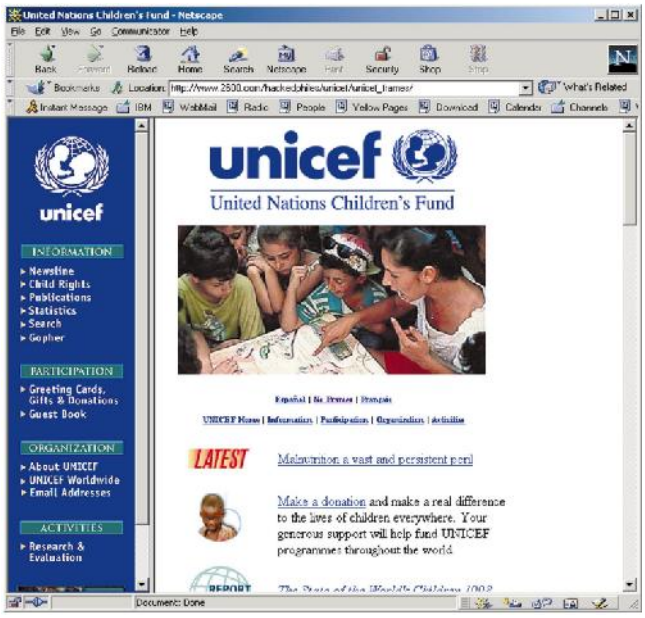

Fig. 3 Página de UNICEF antes del ataque

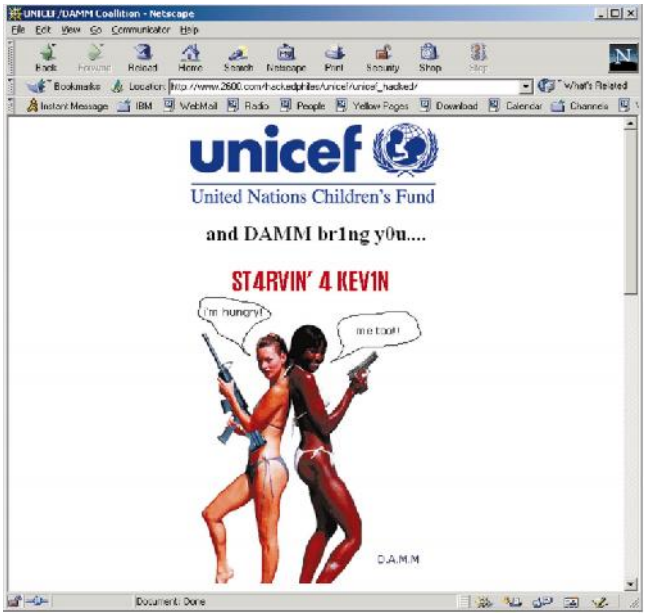

Fig. 4 Página web de UNICEF después del ataque

3. OBJETIVOS DEL HACKING ETICO

Antes que un hacker ético inicie el proceso, se debe crear un plan, como se detalla a continuación:

- Identificar todas y cada una de las redes que probarán.
- Detallar el intervalo de testeo.
- Detallar el proceso de testeo.
- Crear un plan y compartirlo con los clientes involucrados.
- Conseguir que aprueben el plan.

El hackeo ético tiene una variedad de usos en los niveles primario y secundario. Los usos primarios incluyen:

- Garantizar la calidad, usando análisis de tecnologías de seguridad de la información.
- Documentación conforme a regulaciones legales, estándares y parámetros.
- Argumentos de apoyo para actividades de tecnologías de la información y proyectos en el futuro.
- Transferencia Know-how (comprender detalladamente el proceso).
- Conocimiento de infraestructura en todos los niveles.

Los usos primarios y secundarios son básicamente las preguntas que los hackers éticos deben responder, estos incluyen:

- ¿Las mediciones técnicas que se llevan a cabo, se adhieren a los requerimientos legales?
- ¿Hay algún parche que necesite actualizarse y/o está el firewall correctamente configurado?
- ¿Está el servidor de email protegido adecuadamente contra potenciales ataques?
- ¿Todas las medidas de seguridad posibles, han sido implementadas?
- ¿Están adecuadamente seguras el acceso de las oficinas a la red de la compañía?
- ¿Es adecuada la protección contra código malicioso como herramientas de denegación de servicio, troyanos y virus?
- ¿Hay alguna instalación “ilegal”, o todos los sistemas de la compañía están configurados de acuerdo a los estándares?

4. VENTAJAS

La mayoría de los beneficios del hacking ético son obvios, pero muchos son pasados por alto. Los beneficios van desde simplemente prevenir un hacking malicioso a prevenir brechas de seguridad nacional. Los beneficios incluyen:

- **Combatir contra el terrorismo y las brechas de seguridad nacional:** Hay muchas organizaciones terroristas en el mundo que usan la tecnología computacional tratando de crear caos y perjuicios a los gobiernos y organizaciones, un hacking ético minucioso puede anticiparse a estos ataques y prevenir muchos daños.
- **Tener un sistema computacional que evite que los hackers maliciosos obtengan acceso a información restringida:** Como los hackers éticos tienen las mismas herramientas y conocimientos que los hackers criminales, pueden desarrollar medidas preventivas que impidan el acceso a información sensible por parte de cualquier intruso.
- **Tener implementada las medidas preventivas adecuadas para evitar brechas de seguridad:** La seguridad de la información no se trata solo de sistemas computacionales seguros, sino que también es necesario implantar normas y crear conciencia en los trabajadores de la organización sobre la importancia de la seguridad de los datos cruciales.

5. DESVENTAJAS

Como en todo tipo de actividades que tienen un lado oscuro, habrá personas deshonestas que representan un inconveniente. Las posibles desventajas del hacking ético incluyen:

- El hacker ético que usa el conocimiento adquirido del sistema para realizar actividades de hacking criminal.
- Permitir que sean visibles los detalles financieros y banqueros de la compañía.
- La posibilidad de que el hacker ético envíe y/o inserte código malicioso, virus u otro tipo de cosas destructivas y dañinas en el sistema computacional.
- Ruptura de seguridad masiva.

6. CONCLUSIONES

La idea de probar la seguridad de un sistema tratando de irrumpir en ella no es una idea nueva. Ya sea que una compañía de automóviles realice choques entre autos o un individuo pruebe sus habilidades en artes marciales con otro compañero, la evaluación basada en probarse bajo ataque contra un adversario real está ampliamente aceptado como prudente. Esto es sin embargo insuficiente por sí mismo.

Una auditoria regular, vigilancia de intrusiones, una buena práctica de administración de sistemas y una conciencia de la seguridad informática son todos partes esenciales de los esfuerzos de seguridad de una organización. Una pequeña falla en cualquiera de estas áreas muy bien podría exponer a la organización al ridículo, al cyber-vandalismo o algo peor. Cualquier nueva tecnología tiene sus beneficios y sus riesgos.

Aun cuando los hackers éticos pueden ayudar a los clientes a comprender mejor sus necesidades de seguridad, está en manos de los clientes mantener la guardia alta.

7. REFERENCIAS

[1] C.C. Palmer. *Ethical Hacking.* IBM Research Division, Thomas J. Watson Research Center. 2001

[2] Reyes Plata Alejandro. *Ethical Hacking.* UNAM-CERT 2010

[3] Hartley Bruce V *Ethical Hacking: The value of Controlled Penetration Test.* Privisec, Inc. 2003

[4] *Ethical Hacking Student Guide.* Internet Security Systems. Inc. 2000

[5] *Ethical Hacking: Understanding the Benefits, Goals and Disadvantages.* Autor: R. Elizabeth C. Kitchen. Disponible en: http://www.brighthub.com/internet/security-privacy/topics/hacking.aspx

[6] *The Importance of ethical hacking.* Autor: Help Net Security. Disponible en:http://www.net-security.org

[7] *The Benefits of Ethical Hacking.* Autor: Data Central 360. Disponible en:*http://datacentral360.com/the-benefits-of-ethical-hacking/*

[8] *The Benefits of Ethical Hacking.* Autor: Bryan Soliman. Disponible en: *http://bryansoliman.wordpress.com/2011/10/02/the-benefits-of-ethical-hacking/*